REMARKS

Applicants respectfully request reconsideration and allowance of the subject application. Claims 31-40 stand allowed. Claims 6, 17, and 58 are amended. Claims 1-41, 51-60 are provisionally elected. Thus Claims 1-41, 51-60 are pending in this application.

Allowable Subject Matter

Applicants appreciate the allowance of claims 31-40.

The Office Action of 6/21/02 expressly indicates that claims 6, 17, and 58 are allowable. Claims 6, 17, and 58 have been amended in independent form to include all limitations of base claims that are rejected by Examiner. Accordingly, these claims are allowable without further comment or discussion.

Election/Restrictions

Applicants elect to prosecute claims 1-41, 51-60. Claims 42-50 are cancelled without prejudice. Applicants maintain the right to prosecute claims 42-50 in a subsequent application.

CLAIM REJECTIONS

35 U.S.C. § 102

Claims 1, 2, 3, 10, 11, 24, 25-30, and 57 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,341,273 to Briscoe (hereinafter "Briscoe"). Applicants respectfully traverse the rejection.

This invention concerns an electronic asset system and process that captures the efficiency of asset sticks while allowing the flexibility to spend coins from the same stick with multiple vendors. The system is sound, in that the cost to break the system exceeds the maximal possible theft due to the break.

The electronic asset system includes a bank *B* (or other type of issuer), a user *U*, and multiple vendors *V1, V2,... VM*. The system may also include an auditor *A*, although the bank/issuer may perform the auditing functions. The process has four phases: withdrawal, payment, deposit, and audit.

During the withdrawal phase, a user creates a stick of *L* electronic assets by computing:

$$C_i = h^i(x) \quad (\text{for } i{=}1, \ldots, L)$$

where *h(x)* is a hashing function of a value *x*. The user then forms a withdrawal request having a user identity *U*, a user secret *K*, the bottom asset C_L taken from a bottom of the stick, a denomination *d* indicating a value for the assets in the stick, an expiration *t*, and the length *L* (i.e., number of assets in the stick). The user submits the withdrawal request to the bank, which signs the withdrawal request:

$$S_B(U, K, d, C_L, t, L)$$

The bank returns the bank-signed withdrawal request to the user. The resulting stick and signed withdrawal request are not dependent on, nor limited to any vendor. Accordingly, the user is free to spend assets from the stick with different vendors.

During the payment phases, the user decides to spend one or more assets from the stick with a vendor having an identity *V*. The user forms a payment request by concatenating the vendor identity *V*, a first asset *Cj* to be spent from the stick, a depth *D* indicating a distance of the first asset from the bottom of the stick, and a nonce (i.e., a random value generated by the user for inclusion in the payment request). The user signs the payment request:

$$S_U(Cj, D, V1, nonce)$$

The user submits the signed payment request along with the bank-signed withdrawal request to the vendor. The vendor evaluates the signatures of the bank and user and ensures that the coin is properly contained within the stick. If all tests pass, the vendor accepts the first asset as payment. Subsequent to this first asset, the user can pass any additional assets from the stick as payment without digitally signing them.

During the deposit phase, the vendor periodically creates a deposit request having the user-signed first asset $S_U(Cj)$, a last asset spent from the stick *Ck*, and a run length *RL* of assets beginning with the first asset *Cj* and ending with the last asset *Ck*. The vendor signs the deposit request:

$$S_V(S_U(Cj), Ck, RL)$$

The vendor submits the vendor-signed deposit request along with the bank-signed withdrawal request to the bank. The bank evaluates the vendor signature, the user signature, and its own signature. The bank ensures that the assets are from the stick and credits the vendor's account with the run of assets.

During the audit phase, the vendor wallet randomly selects samples of the assets spent by the user and submits the samples to the auditor. The auditor checks whether the assets have been used in a fraudulent manner (i.e. double spent coins). If so, the user identity is revoked. The auditor also employs a deterministic audit that evaluates all spent assets deposited with the bank for purposes of uncovering fraud.

The electronic asset system employs tamper-resistant electronic wallets embodied in a number of different ways, including smart cards, handheld computing devices, and computers. The wallets are constructed as dedicated hardware devices or as devices with secure-processor architecture. The breaking cost of such wallets is higher than the amortized cost of printing or minting false conventional cash. The claims capture this architecture and new technology.

Claim 1 for example recites a method comprising:

> minting a stick of electronic assets by digitally signing with an issuer's signature a composite of user-provided data items including a user identity, a bottom asset from a bottom of the stick, and a length of the stick;
>
> spending one or more assets from the stick at one or more vendors, wherein each expenditure with a particular vendor involves digitally signing with a user's signature a first asset from the stick to be spent and passing the user-signed first asset along with the issuer-signed composite to the particular vendor for verification and subsequently passing any additional assets to be spent without user signature to the particular vendor; and
>
> depositing one or more assets collected by the particular vendor by digitally signing with the particular vendor's signature a composite of data items including the user-signed first asset and a last asset spent by the user

from the stick and passing the vendor-signed composite along with the issuer-signed composite to the issuer.

The method of claim 1 is not disclosed by Briscoe. Briscoe shows a transaction system for use by a broker for minting an electronic coin stick. A client (user) initiates contact with a broker (banker) (Briscoe at col. 5 line 13, Fig. 2). The client requests that the broker issue a coin stick having a specific value, and the client pays for the coin stick (Briscoe at col. 5 lines 19-23). Briscoe does not disclose nor teach that a client is able to mint its own coin stick.

The digitally signed contract of the coin stick in Briscoe includes only coin stick value; coin stick denomination; hash function; coin stick identifier "i" unique within the broker; and an address of the broker's authorization interface (broker URL). (Briscoe at col. 5, lines 43-49). The only identifier that is attached to the coin stick in Briscoe is the coin stick identifier "i" that is unique within the broker (i.e., only the broker is able to differentiate particular coin sticks based on the identifier). The coin stick is issued without being signed with the broker's signature.

A client in Briscoe requests or provides information to the broker for a coin stick of specific value, and a specific denomination. (Briscoe col. 5, lines 19-21). Coin stick value and denomination are two parts of the digitally signed contract. Briscoe does not disclose nor teach that a client provide a client identity in minting the coin stick. Briscoe in fact teaches that "the present invention preserves anonymity" and provides an anonymous payment method (Briscoe at col. 5, 23-25). Attaching a client identity to the coin stick would defeat the object of preserving client anonymity taught in Briscoe.

With a purchased broker-minted coin stick, the client accesses the website of the vendor and begins "spending" assets from the coin stick. This spending involves the transaction module in the vendor calculating the total price of the requested pages by the client and requesting a prepayment of the total price from the client into the vendor payment interface. (Briscoe col. 6, lines 13-16). In the transaction (spending) between client and vendor, Briscoe is silent as to signing a first asset with the user's signature. The vendor in Briscoe does not perform a verification of broker and client signatures, since whatever assets that are presented to the vendor lack client and broker signatures.

In Briscoe, in order to complete a purchase transaction, the vendor connects to the broker's URL, specifically the authorization interface of the broker's URL, pass to the broker the vendor's callback URL and confirm the validity and value of the client's coin stick with the broker (Briscoe at col. 6, lines 31-40). The vendor does not sign whatever assets that are transferred from the client.

Claim 1 recites in part "minting a stick of electronic assets by digitally signing with an issuer's signature a composite of user-provided data items including a user identity." Briscoe does not disclose this aspect. Specifically, Briscoe's methodology does not disclose (1) a user supplying the data items for minting; and (2) having the issuer sign the user provided data items from the stick. As discussed, the broker creates the stick and the only identifier that is shown in Briscoe is a coin stick identifier which is unique only to the broker. The Examiner has pointed out that Briscoe col. 5, lines 44-49 disclose digitally signing with an issuer signature and providing user identity. The section identified by the Examiner includes only the following items in the contract between broker and user: the coin stick value, the coin stick denomination, the hash function, the coin stick identifier, and the broker's authorization interface (URL). This section and the rest of Briscoe are silent as to the requirement of the user supplying data items for minting, and having the issuer sign the user provided data items from the stick.

Claim 1 recites in part "spending one or more assets from the stick at one or more vendors, wherein each expenditure with a particular vendor involves digitally signing with a user's signature a first asset from the stick to be spent and passing the user-signed first asset along with the issuer-signed composite to the particular vendor for verification and subsequently passing any additional assets to be spent without user signature to the particular vendor." Briscoe does not disclose nor teach that the use of a user signature, and in particular a user signature to sign a first asset. As discussed, the issuer never signs the assets. Also as discussed, since the vendor never receives assets signed by an issuer and a user, the vendor is not able to perform verification of the assets based on an issuer-signed composite and subsequent user signature of a first asset or data item. The Examiner asserts that these requirements are found in Briscoe col. 1, lines 63-67 to col. 2 lines 1-24. The section pointed out by the Examiner, as well as the rest of Briscoe, is silent as to a user signature, an issuer signature, and verification of the vendor using user and issuer signatures. Further, Briscoe does not disclose spending assets from the stick with one or more vendors. Briscoe fails to disclose how the same stick could be used with a second vendor. Briscoe would require a different stick to be minted by a broker to be spent with a second vendor. In this respect, Briscoe is akin to the architecture described in the background section of the subject application.

Claim 1 further recites "depositing one or more assets collected by the particular vendor by digitally signing with the particular vendor's signature a composite of data items including the user-signed first asset and a last asset spent by the user from the stick and passing the vendor-signed composite along with the issuer-signed composite to the issuer:" Briscoe does not disclose nor teach a vendor collecting assets by digitally signing the assets with the vendor's signature. A vendor in Briscoe connects with the website of a broker and presents for confirmation the coin stick with identifier "i" unique to the broker having a length of Z_{m+n} (Briscoe col. 6, lines 35-36). Briscoe does not disclose nor teach that the vendor is required to sign the assets that are collected. The Examiner points that this requirement is disclosed in Briscoe col. 6, lines 21-46. This particular section describes the user transacting with a specific vendor; the user calculating from the stick a hash value that is presented and compared by the vendor; and the vendor presenting to the issuer request for payment based on the calculated hash value. This particular section and the rest of Briscoe, however, are silent as to the requirement of a vendor signing assets.

For these reasons, claim 1 is patentable over Briscoe. Applicants respectfully request that the §102 rejection of claim 1 be withdrawn.

Dependent claims 2-5, 7-11 are allowable by virtue of their dependency on base claim 1. For the reasons given above with respect to claim 1, the systems and methods recited in claims 2-5, 7-11 are neither disclosed nor taught by Briscoe. Applicants respectfully request that the §102 rejection of claim 2-5, 7-11 be withdrawn.

Claim 24 recites a method for issuing electronic assets, comprising:

creating, at a user, a stick of L electronic assets by computing:

$$C_i = h^i(x) \quad (\text{for } i=1, \ldots, L)$$

where $h(x)$ is a hashing function of a value x;

submitting a withdrawal request from the user to an issuer, the withdrawal request having a user identity U, a last asset value C_L taken from a bottom of the stick, and the value L, while omitting any vendor identity;

signing, at the issuer, the withdrawal request; and

returning the signed withdrawal request to the user.

The method of claim 24 is not disclosed by Briscoe. Briscoe shows a transaction system for use by a broker for minting an electronic coin stick. A client (user) initiates contact with a broker (banker) (Briscoe at col. 5 line 13, Fig. 2). The client requests that the broker issue a coin stick having a specific value, and the client pays for the coin stick (Briscoe at col. 5 lines 19-23). Briscoe does not disclose nor teach that a client is able to mint its own coin stick

Briscoe fails to disclose "creating, at a user, a stick of L electronic assets" as required by claim 24. Instead, Briscoe discloses that the broker creates the stick. The Examiner points out that Briscoe Fig. 3, col. 3 lines 54-55 disclose creating at a user a stick of L electronic assets. This section describes "generating a hash chain of values which are derived from the secret number." This is described as a method that is performed "at a first party ("the broker")" (Briscoe at col. 3 line 48). This section and the rest of Briscoe fail to describe a user creating the stick.

Briscoe does not disclose "submitting a withdrawal request from the user to an issuer, the withdrawal request having a user identity" as recited by claim 24. The Examiner points to Briscoe at col. 6, lines 21-46 as disclosing a user submitting a withdrawal request from an issuer. This section describes the user transacting with a specific vendor; the user calculating from the stick a hash value that is presented and compared by the vendor; and the vendor presenting to the issuer request for payment based on the calculated hash value. This particular section does not discuss a client or user making a withdrawal request from a broker. Furthermore, the Examiner is inconsistent in his positions. The Examiner has referred to Briscoe at col. 6, lines 21-46 earlier as disclosing "depositing by a vendor." This section as discussed above, describes the transaction between vendor and issuer for the vendor to receive payment from the coin stick presented by a client (user). Further, the rest of Briscoe does not disclose a user submitting a withdrawal request with an issuer.

Briscoe further fails to disclose "signing, at the issuer, the withdrawal request; and returning the signed withdrawal request to the user." The Examiner points to Briscoe at col. 6, lines 21-46 as disclosing this requirement. As discussed above, this section of Briscoe describes the user transacting with a specific vendor; the user calculating from the stick a hash value that is presented and compared by the vendor; and the vendor presenting to the issuer request for payment based on the calculated hash value. This section and the rest of Briscoe fail to disclose an issuer-signed withdrawal request that is returned to the user.

For these reasons, claim 24 is patentable over Briscoe. Applicants respectfully request that the §102 rejection of claim 1 be withdrawn.

Dependent claims 25-30 are allowable by virtue of their dependency on base claim 24. For the reasons given above with respect to claim 1, the systems and methods recited in claims 25-30 are neither disclosed nor taught by Briscoe. Applicants respectfully request that the §102 rejection of claim 25-30 be withdrawn.

35 U.S.C. §103

Claims 4, 15, and 54 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Briscoe in view of U.S. Patent No. 5,878,140 to Chaum (hereinafter "Chaum"). Applicants respectfully traverse the rejection.

Claim 4 depends from claim 1 and hence incorporates the features of claim 1. As such claim 4 requires "minting a stick of electronic assets ... with an issuer's signature a composite of user-provided data items including a user identity ...; spending one or more assets from the stick at one or more vendors, wherein each expenditure with a particular vendor involves digitally signing with a user's signature a first asset from the stick to be spent and passing the user-signed first asset along with the issuer-signed composite to the particular vendor for verification and subsequently passing any additional assets to be spent without user signature to the particular vendor; and depositing one or more assets collected by the particular vendor by digitally signing with the particular vendor's signature a composite of data items including the user-signed first asset ... and passing the vendor-signed composite along with the issuer-signed composite to the issuer."

Briscoe does not suggest nor teach that a stick of electronic assets have an issuer's signature and a user's signature (identity). The coin stick in Briscoe is minted by a broker, and does not provide that a user identity or signature be attached. Briscoe does not suggest nor teach that a vendor signature be attached to assets presented to a broker. A vendor receives payment from a broker by providing only the coin stick with identifier "i" that was created when the broker minted the coin stick (Briscoe at col. 6, lines 35-38).

Chaum is cited for its teaching of a blind protocol. Chaum provides no assistance in light of Briscoe as to the recited methodology of claim 4.

Accordingly, a combination of Briscoe and Chaum fails to teach or suggest the claimed methods. Applicants respectfully request that the §103 rejections of claim 4 be withdrawn.

Claim 15 depends from claim 12 and hence incorporates the features of claim 12. Since claim 15 depends, and incorporates the features of base claim 12, Applicants, initially question whether the rejection of claim 15 over the combination of Briscoe/Chaum is proper given the Examiner's separate rejection of base claim 12 over a different combination of Briscoe and Official Notice.

In any event, since claim 15 depends from claim 12, claim 15 requires "forming a stick of *L* electronic assets C_i (for *i*=1, ..., *L*) where each asset can be derived from a preceding asset in the stick; signing the stick with a signature of a party issuing the assets; spending a first run of one or more assets from the stick at a first vendor; and spending a second run of one or more assets from the stick at a second vendor."

Briscoe does not suggest nor teach a party that forms a stick, sign the stick with the party's (issuer) signature. Although Briscoe discloses an issuer providing an identifier "i", the identifier "i" is unique to the broker and is only used to identify the coin stick to the broker. The identifier "i" is not considered a broker signature (Briscoe at col. 5, line 48). Further, although Briscoe shows a client and vendor performing a transaction, Briscoe is silent as to spending a second run of one or more assets from the stick with a second vendor.

Chaum is cited for its teaching of a blind protocol. Chaum provides no assistance in light of Briscoe as to the recited methodology of claim 15. Accordingly, a combination of Briscoe and Chaum fails to teach or suggest the claimed methods. Applicants respectfully request that the §103 rejections of claims 15 be withdrawn.

Claim 54 depends from claim 51 and hence incorporates the features of claim 51. Since claim 54 depends and incorporates the features of base claim 51, Applicants question the Examiner's rejection of claim 51 over the combination of Briscoe/Chaum, and Examiner's separate rejection of base claim 51 over a combination of Briscoe and Schneier.

Claim 54 depends from claim 51 and hence incorporates the features of claim 51. As such claim 54 requires an issuer wallet with an issuer's signature a composite of user-provided data items including a user identity; a user wallet to store the stick of electronic assets, the user wallet spending one or more assets by signing with a user's signature a first asset to be spent and passing the asset along with the issuer-signed composite to the vendor for verification; whereupon verification, the user wallet subsequently passes any additional assets to be spent without user signature to the vendor; and a vendor wallet having to store one or more assets spent by the user wallet, the vendor wallet depositing the assets collected from the user wallet by signing with the particular vendor's signature a composite of data items including the user-signed asset passed in the stick received from the user wallet and passing the vendor-signed composite along with the issuer-signed composite to the issuer wallet for verification.

Briscoe does not suggest nor teach the use of three separate wallets, an issuer, a user, and a vendor (Briscoe col. 7, lines 57-63). Briscoe shows a smart card that may be used as a hardware wallet for a user; however, Briscoe is silent as to the use of a smart card for a vendor or an issuer. As discussed above, Briscoe does not suggest nor teach the use of signatures of a user, a broker, and vendor. Without signatures of the parties involved, security may be compromised.

Chaum is cited for its teaching of a blind protocol. Chaum provides no assistance in light of Briscoe as to the recited methodology of claim 54. Accordingly, a combination of Briscoe and Chaum fails to teach or suggest the claimed methods. Applicants respectfully request that the §103 rejections of claims 54 be withdrawn.

Claim 5 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Briscoe in view of Official Notice.

Claim 5 depends from claim 1 and hence incorporates the features of claim 1. As such claim 5 requires "minting a stick of electronic assets … with an issuer's signature a composite of user-provided data items including a user identity …; spending one or more assets from the stick at one or more vendors, wherein each expenditure with a particular vendor involves digitally signing with a user's signature a first asset from the stick to be spent and passing the user-signed first asset along with the issuer-signed composite to the particular vendor for verification and subsequently passing any additional assets to be spent without user signature to the particular vendor; and depositing one or more assets collected by the particular vendor by digitally signing with the particular vendor's signature a composite of data items including the user-signed first asset … and passing the vendor-signed composite along with the issuer-signed composite to the issuer."

Applicants assert the arguments made in support of claim 4 above in respect to the requirements outlined by base claim 1.

Official notice is taken that "signing the payment request with a signature of the user" is common and well known in the prior art in reference to electronic money. Applicants traverse such an assertion and request that the Examiner cite a reference in support of his position. If the rejection is based on facts within the personal knowledge of the Examiner, Applicants request an affidavit as provided in MPEP § 2144.03. Nevertheless, the Official Notice taken provides no assistance in light of Briscoe as to the recited methodology of claim 5. Accordingly, a combination of Briscoe and the Official Notice taken fails to teach or suggest the claimed methods. Applicants respectfully request that the §103 rejections of claims 5 be withdrawn.

Claims 7, 8, 9, 19 and 20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Briscoe in view of U.S. Patent No. 5,878,138 to Yacobi (hereinafter "Yacobi"). Applicants respectfully traverse the rejection.

Claims 7, 8, and 9 depend from claim 1 and hence incorporates the features of claim 1. As such claims 7, 8, and 9 require "minting a stick of electronic assets ... with an issuer's signature a composite of user-provided data items including a user identity ...; spending one or more assets from the stick at one or more vendors, wherein each expenditure with a particular vendor involves digitally signing with a user's signature a first asset from the stick to be spent and passing the user-signed first asset along with the issuer-signed composite to the particular vendor for verification and subsequently passing any additional assets to be spent without user signature to the particular vendor; and depositing one or more assets collected by the particular vendor by digitally signing with the particular vendor's signature a composite of data items including the user-signed first asset ... and passing the vendor-signed composite along with the issuer-signed composite to the issuer."

Applicants assert the arguments made in support of claim 4 above in respect to the requirements outlined by base claim 1.

Yacobi is cited for its teaching of auditing the assets from the first and second runs of assets for fraud. Yacobi provides no assistance in light of Briscoe as to the recited methodology of claims 7, 8, and 9. Accordingly, a combination of Briscoe and Chaum fails to teach or suggest the claimed methods. Applicants respectfully request that the §103 rejections of claims 7, 8, and 9 be withdrawn.

Claims 19 and 20 depend from claim 12 and hence incorporate the features of claim 12. As such claims 19 and 20 require "forming a stick of *L* electronic assets C_i (for *i*=1, ..., *L*) where each asset can be derived from a preceding asset in the stick; signing the stick with a signature of a party issuing the assets; spending a first run of one or more assets from the stick at a first vendor; and spending a second run of one or more assets from the stick at a second vendor."

Applicants assert the arguments made in support of claim 15 above in respect to the requirements outlined by base claim 12.

Yacobi is cited for its teaching of auditing the assets from the first and second runs of assets for fraud. Yacobi provides no assistance in light of Briscoe as to the recited methodology of claims 19 and 20. Accordingly, a combination of Briscoe and Chaum fails to teach or suggest the claimed methods. Applicants respectfully request that the §103 rejections of claims 19 and 20 be withdrawn.

Claims 12, 13, 14, 16, 18, 21, 22, and 23 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Briscoe in view of Official Notice. Applicants respectfully traverse the rejection.

Claims 13, 14, 16, 18, 21, 22, and 23 depend from **claim 12** and hence incorporate the features of claim 12. Claim 12 requires "forming a stick of *L* electronic assets C_i (for i=1, ..., L) where each asset can be derived from a preceding asset in the stick; signing the stick with a signature of a party issuing the assets; spending a first run of one or more assets from the stick at a first vendor; and spending a second run of one or more assets from the stick at a second vendor."

As discussed above in support of claim 15, Briscoe does not suggest nor teach a party that forms a stick, sign the stick with the party's (issuer) signature. Although Briscoe discloses an issuer providing an identifier "i", the identifier "i" is unique to the broker and is only used to identify the coin stick to the broker. The identifier "i" is not considered a broker signature. Briscoe at col. 5, line 48. Further, although Briscoe shows a client and vendor performing a transaction, Briscoe is silent as to spending a second run of one or more assets from the stick with a second vendor.

Official notice is taken that "spending a second run of one or more assets from the stick at a second vendor"; "signing the payment request with a signature of the user"; and "depositing the first and second runs of assets" is common and well known in the prior art in reference to electronic money.

Applicants traverse the assertion of Examiner's Official Notice that "spending a second run of one or more assets from the stick at a second vendor" is "well-known" prior art. Further, Applicants traverse that common knowledge in the art would have shown the requirement can be combined with the other requirements of "signing the payment request with a signature of the user"; and "depositing the first and second runs of assets." The background section of the subject application explains that previous systems assign a single coin stick to a single vendor, limiting the user to conduct transactions with only that vendor.

Applicants' system sought to alleviate this limitation of previous systems. Therefore, contrary to the Office's position, it was not well known in the prior art to spend assets from the same stick at multiple vendors. If a user desires to transact with a second vendor, the user must contact the broker (issuer) to issue a new stick that identifies the second vendor. If the Office maintains the rejection, Applicants request that the Examiner cite a reference in support of this position. If the rejection is based on facts within the personal knowledge of the Examiner, Applicants request an affidavit as provided in MPEP § 2144.03. Nevertheless, the Official Notice taken provides no assistance in light of Briscoe as to the recited methodology of claim 12, 13, 14, 16, 18, 21, 22, and 23. Accordingly, a combination of Briscoe and the Official Notice taken fails to teach or suggest the claimed methods. Applicants respectfully request that the §103 rejections of claims 12, 13, 14, 16, 18, 21, 22, and 23 be withdrawn.

Claims 51-53 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Briscoe in view of "Applied Cryptography" by Schneier (hereinafter "Schneier"). Applicants respectfully traverse the rejection.

Claims 52-53 depend from **claim 51** and hence incorporate the features of claim 51. Claim 51 requires an issuer wallet having a with an issuer's signature a composite of user-provided data items including a user identity; a user wallet to store the stick of electronic assets, the user wallet spending one or more assets by signing with a user's signature a first asset to be spent and passing the asset along with the issuer-signed composite to the vendor for verification; whereupon verification, the user wallet subsequently passes any additional assets to be spent without user signature to the vendor; and a vendor wallet having to store one or more assets spent by the user wallet, the vendor wallet depositing the assets collected from the user wallet by signing with the particular vendor's signature a composite of data items including the user-signed asset passed in the stick received from the user wallet and passing the vendor-signed composite along with the issuer-signed composite to the issuer wallet for verification.

Applicants assert the arguments made in support of claim 54 above in respect to the requirements outlined by base claim 51.

Schneier is cited for its teaching of message transmission in order to prevent adversaries from forging electronic asset transactions. Schneier provides no assistance in light of Briscoe as to the recited methodology of claims 51-53. Accordingly, a combination of Briscoe and Schneier fails to teach or suggest the claimed methods. Applicants respectfully request that the §103 rejections of claims 51-53 be withdrawn.

Claims 55-56 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Briscoe in view of U.S. Patent No. 6,021,399 to Deemers et al (hereinafter "Deemers"). Applicants respectfully traverse the rejection.

Claims 55-56 depend from **claim 51** and hence incorporate the features of claim 51.

Applicants assert the arguments made in support of claim 54 above in respect to the requirements outlined by base claim 51.

Deemers is cited for its teaching of "an auditing system to audit the electronic assets to detect whether assets have been used in a fraudulent manner" and "a probabilistic auditing system to sample a subset of less than all electronic assets, to detect whether assets have been used in a fraudulent manner." Deemers provides no assistance in light of Briscoe as to the recited methodology of claims 55-56. Accordingly, a combination of Briscoe and Deemers fails to teach or suggest the claimed methods. Applicants respectfully request that the §103 rejections of claims 55-56 be withdrawn.

Claims 59-60 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Briscoe in view of Yacobi. Applicants respectfully traverse the rejection.

Claim 60 depends from **claim 59** and hence incorporates the features of claim 59. Claim 59 requires an electronic wallet having memory and a processor, the electronic wallet being programmed to: receive a run of assets from a user; select a subset of less than all of the assets received from the user; and submit the subset of assets to an auditor for evaluation of fraudulent expenditure."

Examiner admits that Briscoe does not disclose an electronic wallet to receive a run of assets from a user, select a subset of less than all of the assets received from the user; and submit the subset of assets to an auditor for evaluation of fraudulent expenditure.

Yacobi is cited for its teaching of "an electronic wallet to receive a run of assets from a user, select a subset of less than all of the assets received from the user; and submit the subset of assets to an auditor for evaluation of fraudulent expenditure"; however, Examiner has not particularly pointed out an electronic wallet in Yacobi that receives a run of assets. Examiner further has not particularly pointed out in Yacobi where a subset of assets are presented to an auditor for fraudulent expenditure. Accordingly, a combination of Briscoe and Yacobi fails to teach or suggest the claimed methods. Applicants respectfully request that the §103 rejections of claims 59 and 60 be withdrawn.

Claim 60 which depends on claim 59 further recites in part "further programmed to randomly select the subset of assets."

CONCLUSION

All pending claims 1-41, 51-60 are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the subject application. If any issues remain that prevent issuance of this application, the Examiner is urged to contact the undersigned attorney before issuing a subsequent Action.

Respectfully Submitted,

Date: 11/19/02

By: ______________________
Emmanuel A. Rivera
Reg. No. 45,760
(509) 324-9256 ext. 245

MARKED UP VERSION OF PENDING CLAIMS UNDER 37 C.F.R. 1.121(C)(1)(ii):

Amend claims 6, 17, and 58 as follows and in accordance with 37 C.F.R.. 1.121(c)(1)(ii), by which the Applicant submits the following marked up version only for claims being changed by the current amendment, wherein the markings are shown by brackets (for deleted matter) and/or underlining (for added matter):

6. (Amended Once) A method [as recited in claim 1]comprising:

minting a stick of electronic assets by digitally signing with an issuer's signature a composite of user-provided data items including a user identity, a bottom asset from a bottom of the stick, and a length of the stick;

spending one or more assets from the stick at one or more vendors, wherein each expenditure with a particular vendor involves digitally signing with a user's signature a first asset from the stick to be spent and passing the user-signed first asset along with the issuer-signed composite to the particular vendor for verification and subsequently passing any additional assets to be spent without user signature to the particular vendor; and

depositing one or more assets collected by the particular vendor by digitally signing with the particular vendor's signature a composite of data items including the user-signed first asset and a last asset spent by the user from the stick and passing the vendor-signed composite along with the issuer-signed composite to the issuer, wherein the depositing comprises:

concatenating the user-signed first asset $S_U(Cj)$, a last asset spent from the stick Ck, and a run length RL of assets beginning with the first asset Cj and ending with the last asset Ck to form a deposit request;

signing the deposit request with a signature of the vendor:

$$S_V(S_U(Cj), Ck, RL)$$

submitting the vendor-signed deposit request along with the issuer-signed withdrawal request to the issuer; and

crediting a vendor account with the run of assets in an event that the user, the vendor, the run, and the issuer are positively verified.

17. (Amended Once) A method [as recited by claim 16]for issuing electronic assets, comprising:

forming a stick of L electronic assets C_i (for i=1, ..., L) where each asset can be derived from a preceding asset in the stick; wherein the forming [further] comprises:

creating the stick of L electronic assets by computing:

$$C_i = h^i(x) \quad \text{(for } i=1, \ldots, L)$$

where $h(x)$ is a one-way hashing function of a value x;

constructing a withdrawal request having a user identity U, a user secret K, a last asset value C_L taken from a bottom of the stick, a denomination d indicating a value for the assets in the stick, an expiration t, and the value L; and

signing the withdrawal request with a signature of an issuer:

$$S_I(U, K, d, C_L, t, L)[.];$$

signing the stick with a signature of a party issuing the assets;

spending a first run of one or more assets from the stick at a first vendor; and

spending a second run of one or more assets from the stick at a second vendor.

58. An electronic wallet [as recited in claim 57, further] having memory and a processor, the electronic wallet being programmed to:

create a stick of L electronic assets by computing:

$$C_i = h^i(x) \quad (\text{for } i=1, \ldots, L)$$

where $h(x)$ is a hashing function of a value x;

form a withdrawal request having a user identity U, a last asset value C_L taken from a bottom of the stick, and the value L, while omitting any vendor identity;

submit withdrawal request to an issuer and receive the withdrawal request back with an issuer signature;

store the signed withdrawal request and the stick;

form a payment request for payment of one or more assets from the stick to a vendor having an identity V, the payment request having the vendor identity V and a first asset Cj to be spent from the stick;

sign the payment request:

$S_U(Cj, V1)$; and

submit the signed payment request along with the signed withdrawal request to the vendor.

MARKED UP VERSION OF SPECIFICATION UNDER 37 C.F.R. § 1.121(B)(1)(iii):

Page 18, third paragraph

At step 102, the vendor sends the signed deposit request along with the signed withdrawal request to the [vendor]bank.

Page 26, fourth paragraph

Fig. 7 shows the linked dual-stick data structure 200 having a user stick 202 and a vendor stick 204. Each stick is configured according to a FIFO (first in first out) policy, where earned coupons are added to the top of the stick and spent coupons are removed from the bottom of the stick. Each stick has two pointers: a top pointer *Pt* and a bottom pointer *Pb*. As coupons are added, the top pointer *Pt* is incremented to reflect new coupons that are now available for use. As coupons are spent, the bottom pointer *Pb* is incremented to reflect their expenditure and reference the next unused coupon in the stick to be spent. The balance of available coupons, *B*, is equal to the difference between the top and bottom pointers (i.e., *B=Pt-Pb*).

DRAWINGS UNDER 37 C.F.R. § 1.121(D)

Drawing changes are submitted for Fig. 5, and are provided separately.